UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,784	12/24/2003	Harold J. Johnson	201371-05000	6160

41018 7590 06/25/2008

CASSAN MACLEAN
307 GILMOUR STREET
OTTAWA, ON K2P 0P7
CANADA

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/743,784	JOHNSON ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 31-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 31-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 03/07/2008. In light of the applicant's amendments, the examiner hereby withdraws his previous Claim Objections regarding Claims 5, 8, & 26 and his previous 35 U.S.C. 112 2nd paragraph regarding Claim 6. Claims 1 & 31-37 are pending and have been considered as follows.

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

- Claim 35 line 2 recites, "a random form," however, it appears that the applicant's Specification does not provide support for this limitation;

Claim Objections

2. Claim 1 is objected to because of the following informalities:

- Claim 1 line 2 recites the term "for" which should be "…configured to…";

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 35 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- Claim 35 line 2 recites, "a random form," however, it appears that the applicant's Specification does not provide support for this limitation and is considered new matter;

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shinn (US-6655585-B2) in view of Collberg et al. (US-6668325-B1).

- The examiner notes that for the considerations below, it appears based on the examiner's broadest most reasonable interpretation, that the applicant's limitations, Claim 1 limitations in particular, are directed towards mere biometric template comparison verification and typical software code obfuscation and tamper prevention techniques;

despite the additional details in the applicant's Specification which describe the software code obfuscation/TSR in greater detail than is currently claimed; in addition, the examiner also notes additional details not claimed for the applicant's limitations reciting what appears to be nothing more than varying degrees or levels of security desired based on different TSR encoding techniques;

Claim 1:

Shinn discloses a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft comprising,

- "establishing parameters of the access software application" (i.e. "When the person attempts to access the system, the application collects new data") [column 1 lines 37-38];
- "generating a biometric template for a user by sampling" (i.e. "A person enrolls by donating some number of samples of the biometric. From these samples, the biometric system creates a model of the particular individual's patterns, which is referred to as a template") [column 1 lines 34-37];
- "employing the biometric template which has been integrated into the access software application to evaluate biometric data provided by a user seeking to access the other application, system or software entity to provide an evaluation result which either permits or denies access by the user" (i.e. "In a verification application, the individual claims an identity, and the application retrieves the individual's model from a database and compares the new signal to the retrieved model. The result of this comparison is a match score, which indicates how well the new signal matches the template. The application

then compares the match score obtained with a pre-defined threshold and decides whether to allow or deny access to the individual or, for example, to ask the individual for more data.") [column 1 lines 39-48];

but, Shinn does not explicitly disclose,

- "integrating into the access software application by means of partial evaluation, the parameters and the biometric template," although Collberg et al. do suggest utilizing partial evaluation for software protection, as recited below;
- "performing tamper-resistant software (TRS) encoding to the access software application according to one of the following: prior to the establishing of parameters, whereby one TRS implementation covers multiple platforms and multiple biometric templates," although Collberg et al. do suggest applying code obfuscation techniques including varying degrees of security dependent on the algorithms and transformations used for the desired level of potency, execution time/space, and cost, as recited below;
- "after the establishing of parameters and before generating the biometric template, whereby one TRS implementation covers one platform only and multiple biometric templates," although Collberg et al. do suggest applying code obfuscation techniques including varying degrees of security dependent on the algorithms and transformations used for the desired level of potency, execution time/space, and cost, as recited below;

- "after the establishing of parameters and after generating the biometric template, whereby one TRS implementation covers one platform only and one biometric template only," although Collberg et al. do suggest applying code obfuscation techniques including varying degrees of security dependent on the algorithms and transformations used for the desired level of potency, execution time/space, and cost, as recited below;

however, Collberg et al. do disclose,

- "Deobfuscation also resembles partial evaluation. A partial evaluator splits a program into two parts: the static part which can be precomputed by the partial evaluator, and the dynamic part which is executed at runtime. The dynamic part would correspond to our original, unobfuscated, program. The static part would correspond to our bogus inner program, which, if it were identified, could be evaluated and removed at deobfuscation time" [column 31 lines 46-53];
- " FIG. 6 shows an architecture of Kava, the Java obfuscator. The main input to the tool is a set of Java class files and the obfuscation level required by the user. The user may optionally provide files of profiling data, as generated by Java profiling tools. This information can be used to guide the obfuscator to make sure that frequently executed parts of the application are not obfuscated by very expensive transformations. Input to the tool is a Java application, given as a set of Java class files. The user also selects the required level of obfuscation (e.g., potency) and the maximum execution time/space penalty that the obfuscator is allowed to add to the application (the cost)" [column 10 lines 57-67 & column 11 line 1];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "integrating into the access software application by means of partial evaluation, the parameters and the biometric template" and "performing tamper-resistant software (TRS) encoding to the access software application according to one of the following: prior to the establishing of parameters, whereby one TRS implementation covers multiple platforms and multiple biometric templates" and "after the establishing of parameters and before generating the biometric template, whereby one TRS implementation covers one platform only and multiple biometric templates" and "after the establishing of parameters and after generating the biometric template, whereby one TRS implementation covers one platform only and one biometric template only," in the invention as disclosed by Shinn for the purposes of providing various degrees of security through software code obfuscation.

7. Claims 31 & 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinn (US-6655585-B2) in view of Collberg et al. (US-6668325-B1) and in further view of Kaliski, Jr. (US-6085320-A).

Claim 31:

Shinn and Collberg et al. disclose a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft, as in Claim 1 above, but their combination do not explicitly disclose,

- "whereby the evaluation result comprises a cryptographic key generated to be either correct to permit access by the user or incorrect to deny access by the user," although Kaliski, Jr. does suggest utilizing a well known protocol for proving authenticity involving keys, as recited below;
- "the cryptographic key being generated to be correct only when the user-provided biometric data is found to match the biometric template," although Kaliski, Jr. does suggest public key/private key, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "whereby the evaluation result comprises a cryptographic key generated to be either correct to permit access by the user or incorrect to deny access by the user"

and "the cryptographic key being generated to be correct only when the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Shinn and Collberg et al. for the purposes of providing additional security through key encryption.

Claim 33:

Shinn, Collberg et al., and Kaliski, Jr. disclose a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft, as in Claim 31 above, but the combination of Shinn and Collberg et al. do not explicitly disclose,

- "whereby the evaluation result comprises a key for a symmetric cipher having high entropy for its key length, if the user-provided biometric data is found to match the biometric template," although Kaliski, Jr. does suggest public key/private key encryption, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "whereby the evaluation result comprises a key for a symmetric cipher having high entropy for its key length, if the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Shinn and Collberg et al. for the purposes of providing additional security through public key/private key encryption.

Claim 34:

Shinn, Collberg et al., and Kaliski, Jr. disclose a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft, as in Claim 31 above, but the combination of Shinn and Collberg et al. do not explicitly disclose,

- "whereby the evaluation result comprises private key of a public/private key pair, if the user-provided biometric data is found to match the biometric template," although Kaliski, Jr. does suggest public key/private key encryption, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This

message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "whereby the evaluation result comprises private key of a public/private key pair, if the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Shinn and Collberg et al. for the purposes of providing additional security through public key/private key encryption.

Claim 35:

Shinn and Collberg et al. disclose a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft, as in Claim 1 above, but their combination do not explicitly disclose,

- "whereby the evaluation result comprises a random form if the user-provided biometric data is found not to match the biometric template," although Kaliski, Jr. does suggest utilizing a time varying message encrypted according to a public key/private key encryption scheme, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a digital signature with its private key on a time-varying message, and the server verifies

> the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "whereby the evaluation result comprises a random form if the user-provided biometric data is found not to match the biometric template," in the invention as disclosed by Shinn and Collberg et al. for the purposes of protecting information/data through the use of unique time varying information.

Claim 36:

Shinn, Collberg et al., and Kaliski, Jr. disclose a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft, as in Claim 31 above, but the combination of Shinn and Collberg et al. do not explicitly disclose,

- "whereby the incorrect cryptographic key is identical in bit-length to the correct cryptographic key," although Kaliski, Jr. does suggest utilizing public key/private key encryption with a time varying message and digital signature, as recited below;

however, Kaliski, Jr. does disclose,

- "A standard well known protocol for proving authenticity involves public-key cryptography. The client establishes a public key/private key pair and provides the public key to the server. In a transaction, to prove its authenticity to the server, the client forms a

digital signature with its private key on a time-varying message, and the server verifies the digital signature with the client's public key. The time-varying message, which may be a timestamp or a challenge supplied by the server, is different in each instance. This message, when checked by the server, provides safeguards against a third party impersonating the client by simply replaying copies of previous signatures of the client that the third party has intercepted or otherwise acquired" [column 1 lines 24-36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "whereby the incorrect cryptographic key is identical in bit-length to the correct cryptographic key," in the invention as disclosed by Shinn and Collberg et al. for the purposes of providing safe guard against replay attacks.

8. Claims 32 & 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinn (US-6655585-B2) in view of Collberg et al. (US-6668325-B1) and in further view of Chow et al. (US-6779114-B1).

Claim 32:

Shinn and Collberg et al. disclose a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft, as in Claim 1 above, but their combination do not explicitly disclose,

- "whereby the evaluation result comprises branching to a distinct location of the access software application if the user-provided biometric data is found to match the biometric template," although Chow et al. does suggest control flow encoding, as recited below;

however, Chow et al. does disclose,

- "Control-flow describes the manner in which execution progresses through the software code. The invention increases the complexity of the control flow by orders of magnitude, obscuring the flow of its algorithm and preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 8-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "whereby the evaluation result comprises branching to a distinct location of the access software application if the user-provided biometric data is found to match the biometric template," in the invention as disclosed by Shinn and Collberg et al. for the purposes of providing tamper resistance by control flow encoding.

Claim 37:

Shinn and Collberg et al. disclose a method of biometric verification using an access software application for accessing another application, system or other software entity to protect biometric data against spoofing or theft, as in Claim 1 above, but their combination do not explicitly disclose,

- "whereby the TRS encoding comprises mass data encoding for data in array, table or message buffer form," although Chow et al. does suggest mass data encoding, as recited below;

however, Chow et al. does disclose,

- "If a large number of control transfers are added to the software code, it will be extremely difficult for the attacker to identify the specific line of control that he wishes to modify" [column 12 lines 23-26];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "whereby the TRS encoding comprises mass data encoding for data in array, table or message buffer form," in the invention as disclosed by Shinn and Collberg et al. for the purposes of providing tamper resistance by mass data encoding.

Response to Arguments

9. Applicant's arguments with respect to claims 1 & 31-37 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
06/18/2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136